UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/672,496	09/29/2000	Ernie F. Brickell	PM 271382	2631

27496 7590 02/11/2004

PILLSBURY WINTHROP LLP
725 S. FIGUEROA STREET
SUITE 2800
LOS ANGELES, CA 90017

EXAMINER	
BETIT, JACOB F	
ART UNIT	**PAPER NUMBER**
2175	7

DATE MAILED: 02/11/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/672,496	BRICKELL ET AL.	
	Examiner	Art Unit	
	Jacob F. Betit	2175	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-28* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *29 September 2000* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

13)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

a) ☐ The translation of the foreign language provisional application has been received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

DOV POPOVICI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____.
4) ☐ Interview Summary (PTO-413) Paper No(s). _____
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other:

DETAILED ACTION

Drawings

1. The drawings are objected to because Hash1 of figure 3, step 302 is said to equal hash(PWD, UserName, Salt2). Because Hash1 was equated to hash(PWD, UserName, Salt1) in both figure 2, step 205 and on page 6, lines 21-25 in the disclosed specification, for the purposes of examination, the examiner is making the assumption that the applicant meant Hash1= hash(PWD, UserName, Salt1). A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

Specification

2. The arrangement of the disclosed application does not conform with 37 CFR 1.77(b).

Section headings are boldfaced throughout the disclosed specification, and "Field of the Invention" and "Description of Related Art" do not appear in upper case lettering. Section headings should not be underlined and/or **boldfaced**, and they should appear in upper case lettering. Appropriate corrections are required according to the guidelines provided below:

3. The following guidelines illustrate the preferred layout for the specification of a utility application. These guidelines are suggested for the applicant's use.

Arrangement of the Specification

As provided in 37 CFR 1.77(b), the specification of a utility application should include the following sections in order. Each of the lettered items should appear in upper case, without underlining or bold type, as a section heading. If no text follows the section heading, the phrase "Not Applicable" should follow the section heading:

(a) TITLE OF THE INVENTION.
(b) CROSS-REFERENCE TO RELATED APPLICATIONS.
(c) STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT.
(d) INCORPORATION-BY-REFERENCE OF MATERIAL SUBMITTED ON A COMPACT DISC (See 37 CFR 1.52(e)(5) and MPEP 608.05. Computer program listings (37 CFR 1.96(c)), "Sequence Listings" (37 CFR 1.821(c)), and tables having more than 50 pages of text are permitted to be submitted on compact discs.) or
REFERENCE TO A "MICROFICHE APPENDIX" (See MPEP § 608.05(a). "Microfiche Appendices" were accepted by the Office until March 1, 2001.)
(e) BACKGROUND OF THE INVENTION.
(1) Field of the Invention.
(2) Description of Related Art including information disclosed under 37 CFR 1.97 and 1.98.
(f) BRIEF SUMMARY OF THE INVENTION.
(g) BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWING(S).
(h) DETAILED DESCRIPTION OF THE INVENTION.
(i) CLAIM OR CLAIMS (commencing on a separate sheet).
(j) ABSTRACT OF THE DISCLOSURE (commencing on a separate sheet).
(k) SEQUENCE LISTING (See MPEP § 2424 and 37 CFR 1.821-1.825. A "Sequence Listing" is required on paper if the application discloses a nucleotide or amino acid sequence as defined in 37 CFR 1.821(a) and if the required "Sequence Listing" is not submitted as an electronic document on compact disc).

Claim Objections

4. Claims 8 and 17 are objected to because of the following informalities: Claim 8 ends with a semicolon instead of a period. Claim 17 ends without any kind of punctuation. Each claim should end with a period.

Appropriate correction is required.

Claim Rejections - 35 USC § 112

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claims 6, 9, and 10 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

7. Claims 6, in line 5, and 9, in line 6, recite the limitation "the private key". There is insufficient antecedent basis for these limitations in the claim. For the purpose of examining, the examiner is making the assumption the applicant meant "the private information" not "the private key".

Claim 10 is rejected as being dependant on rejected dependent claim 9.

Appropriate correction is required.

Claim Rejections - 35 USC § 102

8. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

9. Claims 11-12 and 14-15 are rejected under 35 U.S.C. 102(e) as being anticipated by Gurevich et al. (U.S. patent application publication No. 2002/0178370 A1).

As to claim 11, Gurevich et al. teaches a method of deriving private information (see abstract) of a user comprising:

receiving a first value from a key server located remotely from the user, the first value being related to the private information (see page 6, paragraph 0070, line 2-6);

retrieving a second value stored on a computer system of the user (see page 6, paragraph 0068, line 6-10, and see paragraph 0070, lines 6-10); and

calculating the private information based on the first and second values (see page 6, paragraph 0070, line 6-11).

As to claim 12, Gurevich et al. teaches wherein the calculation of the private information additionally includes using a password of the user to calculate the private information (see figure 1, decryption, and see encryption, line 2).

As to claim 14, Gurevich et al. teaches further comprising authenticating the user of the private information at the remote key server (see figure 1, authentication).

As to claim 15, Gurevich et al. teaches wherein the method of authenticating is using a biometric device (see page 5, paragraph 0059).

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. Claims 1-10, 13, 16-18, 20, and 22-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gurevich et al. (U.S. patent application publication No. 2002/0178370 A1) in view of Dolan et al. (U.S. patent No. 5,604,801).

As to claim 1, Gurevich et al. teaches method for securing private information

(see abstract), comprising:

calculating a first value and a second value which together are needed to derive the private information (see page 6, paragraph 0068); and

registering the first value with a remote server (see page 6, paragraph 0068, lines 13-18).

Gurevich et al. does not teach securely storing the second value in a local client memory that is independent of the remote server; and deleting the first value from the local client memory.

Dolan et al. teaches securely storing the second value in a local client memory that is independent of the remote server; and deleting the first value from the local client memory (see column 9, lines 55-58).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Gurevich et al. to include securely storing the second value in a local client memory that is independent of the remote server; and deleting the first value from the local client memory.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Gurevich et al. by the teachings of Dolan et al. because securely storing the second value in a local client memory that is independent of the remote server; and deleting the first value from the local client memory would allow only the authorized holder of a device to process a message (see Dolan et al., column 2, lines 54-64).

As to claim 2, Gurevich et al. as modified, does not teach wherein the private information is a private key in a public/private key pair.

Dolan et al. teaches wherein the private information is a private key in a public/private key pair (see abstract).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Gurevich et al. as modified, to include wherein the private information is a private key in a public/private key pair.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Gurevich et al. as modified, by the teachings of Dolan et al. because wherein the private information is a private key in a public/private key pair would allow only the authorized holder of a device to process a message (see Dolan et al., column 2, lines 54-64).

As to claim 3, Gurevich et al. as modified, teaches additionally including registering an authentication value with the remote server (see Gurevich et al., page 5, paragraph 0058).

As to claim 4, Gurevich et al. as modified, teaches wherein a password provided by a user of the private information is needed to derive the private information in addition to the first value and the second value (see Gurevich et al., figure 1, decryption and see figure 1, encryption, line 2, where "password" is read on "PIN").

As to claim 5, Gurevich et al. as modified, teaches wherein calculating the first and second values includes:

generating a random value (see Gurevich et al., page 6, paragraph 0068, lines 3-6);

deriving the first value from the random value (see Gurevich et al., page 6, paragraph 0068, lines 3-6); and

deriving the second value from the private information and the random value (see Gurevich et al., page 6, paragraph 0068, line 6-13).

As to claim 6, Gurevich et al. as modified teaches wherein calculating the first and second values includes:

generating a random value as the first value(see Gurevich et al., page 6, paragraph 0068, lines 3-6);

deriving a wrapping encryption key from the first value (see Gurevich et al., page 6, paragraph 0068, lines 3-12); and

encrypting the private information with the wrapping encryption key to form the second value (see Gurevich et al., page 6, paragraph 0068, line 6-13).

As to claim 7, Gurevich et al., teaches a method of securing private information (see abstract) comprising:

entering a password (see page 5, paragraph 0064, lines 2-7, where "password" is read on "PIN");

calculating a first value and a second value (see page 6, paragraph 0068) and storing the first value and the second value in a local client memory (see page 6, paragraph 0070, lines 6-11, and see page 6, paragraph 0074, lines 3-6), the first and second values together with the password being needed to derive the private information (see figure 1, authentication and decryption);

calculating an authentication value from the password (see figure 1, authentication); and

registering the first value (see page 6, paragraph 0068, line 13-18) and the authentication value with a remote key server (see page 5, paragraph 0058, where it is obvious that an "authentication value" must be registered with the "remote key server" in order for it to provide for user authentication).

Gurevich et al. does not teach deleting the first value from the local client memory.

Dolan et al. teaches deleting the first value from the local client memory (see column 9, lines 55-58).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Gurevich et al. to include deleting the first value from the local client memory.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Gurevich et al. by the teachings of Dolan et al. because deleting the first value from the local client memory would allow only the authorized holder of a device to process a message (see Dolan et al., column 2, lines

54-64).

As to claim 8, Gurevich et al. as modified, teaches wherein calculating the first value and the second value includes:

generating a random value (see Gurevich et al., page 6, paragraph 0068, line 3-6);

generating a first fixed value and a second fixed value (see Gurevich et al., page 5, paragraph 0057, where generating a second fixed value is obvious to one skilled in the art to make the wrapped private information harder to decrypt);

deriving the first value from the random value, the password, a user name, and the first fixed value (see Gurevich et al., page 6, paragraph 0068, line 3-9, where the token is used both as the "first fixed value" and "a user name" because it is a long random string that will identify the current user); and

deriving the second value from the private information, the random value, the password, the user name, and the second fixed value (see Gurevich et al., page 6, paragraph 0068, line 3-13).

As to claim 9, Gurevich et al. as modified, teaches wherein calculating the first value and the second value includes:

generating a random value as the first value (see Gurevich et al., page 6, paragraph 0068, line 3-6);

deriving a wrapping encryption key from the first value, the password, and a user

name (see Gurevich et al., page 6, paragraph 0068, line 3-12); and

encrypting the private information with the wrapping encryption key to form the second value (see Gurevich et al., page 6, paragraph 0068, line 6-13).

As to claim 10, Gurevich et al. as modified, teaches wherein the authentication value is calculated by:

generating a fixed value (see Gurevich et al., page 5, paragraph 0057); and

deriving the authentication value from the fixed value, the password, and the user name (see Gurevich et al., figure 1, where token key is read on user name).

As to claim 13, Gurevich et al. does not teach wherein the private information is a private key in a public key cryptographic system.

Dolan et al. teaches wherein the private information is a private key in a public key cryptographic system (see abstract).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Gurevich et al. to include wherein the private information is a private key in a public key cryptographic system.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Gurevich et al. by the teachings of Dolan et al. because wherein the private information is a private key in a public key cryptographic system would allow only the authorized holder of a device to process a message (see Dolan et al., column 2, lines 54-64).

As to claim 16, Gurevich et al. teaches a method comprising:

wrapping the first number using a symmetric encryption key derived from a password entered by a user of the private key (see page 6, paragraph 0068, line 6-13); and

registering the wrapped version of the first number with a remote key server (see page 6, paragraph 0068, line 13-18).

Gurevich et al. does not teach generating a public key and a corresponding private key for a public key cryptographic system; and calculating a first number based on the private key and a random number.

Dolan et al. teaches generating a public key and a corresponding private key for a public key cryptographic system (see column 9, lines 31-38); and calculating a first number based on the private key and a random number (see column 9, lines 45-49).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Gurevich et al. to include generating a public key and a corresponding private key for a public key cryptographic system; and calculating a first number based on the private key and a random number.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Gurevich et al. by the teachings of Dolan et al. because generating a public key and a corresponding private key for a public key cryptographic system; and calculating a first number based on the private key and a

random number would allow only the authorized holder of a device to process a message (see Dolan et al., column 2, lines 54-64).

As to claim 17, Gurevich et al. as modified, teaches wherein the symmetric encryption key is derived from a first hash value based on the password, a user name, and a first fixed random number (see Gurevich et al., page 6, paragraph 0068, line 3-12, where "user name" is read on "token key" and "first fixed random number" is read on "SKP").

As to claim 18, Gurevich et al. teaches a computer system (see page 8, paragraph 0107) comprising:

a processor (see page 8, paragraph 0107, line 5-8); and

a computer memory connected to the processor (see pages 8-9, paragraph 108) and wrap the first number using a symmetric encryption key derived from a password entered by a user of the private key (see page 6, paragraph 0068, line 6-13); wherein

the wrapped version of the first number is registered with a remote server (see page 6, paragraph 0068, line 13-18), the computer system retrieving the wrapped version of the first number before initiating a secure communication session using the private key (see page 6, paragraph 0070, line 3-6).

Gurevich et al. does not teach the computer memory including a cryptographic program configured to generate a public key and a corresponding private key for a public key cryptographic system; and the wrapped version then deleted from the

computer system.

Dolan et al. teaches the computer memory including a cryptographic program configured to generate a public key and a corresponding private key for a public key cryptographic system (see column 9, lines 32-38); calculate a first number based on the private key and a random number (see column 9, lines 45-49); and the wrapped version then deleted from the computer system (see column 9, lines 55-58).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Gurevich et al. to include the computer memory including a cryptographic program configured to generate a public key and a corresponding private key for a public key cryptographic system; and the wrapped version then deleted from the computer system.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Gurevich et al. by the teachings of Dolan et al. because the computer memory including a cryptographic program configured to generate a public key and a corresponding private key for a public key cryptographic system; and the wrapped version then deleted from the computer system would allow only the authorized holder of a device to process a message (see Dolan et al., column 2, lines 54-64).

As to claim 20, Gurevich et al. as modified, teaches wherein the symmetric encryption key is derived from a first hash value based on the password, a user name, and a first fixed random number (see Gurevich et al., page 6, paragraph

0068, line 3-12, where "user name" is read on "token key" and "first fixed random number" is read on "SKP").

As to claim 22, Gurevich et al. teaches a computer readable medium containing instructions for execution by a processor (see page 3, paragraph 0028), the instructions, when executed:

wrap the first number using a symmetric encryption key derived from a password entered by a user of the private key (see page 6, paragraph 0068, line 6-13); and

registering the wrapped version of the first number with a remote key server (see page 6, paragraph 0068, line 13-18).

Gurevich et al. does not teach generate a public key and a corresponding private key for a public key cryptographic system.

Dolan et al. teaches generate a public key and a corresponding private key for a public key cryptographic system (see column 9, lines 32-38); and calculate a first number based on the private key and a random number (see column 9, lines 45-49).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Gurevich et al. to include generate a public key and a corresponding private key for a public key cryptographic system.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Gurevich et al. by the teachings of Dolan et al. because generate a public key and a corresponding private key for a public key cryptographic system would allow only the authorized holder of a device to process a

message (see Dolan et al., column 2, lines 54-64).

As to claim 23, Gurevich et al. as modified, teaches wherein the symmetric encryption key is derived from a first hash value based on the password, a user name, and a first fixed random number (see Gurevich et al., page 6, paragraph 0068, line 3-12, where "user name" is read on "token key" and "first fixed random number" is read on "SKP").

12. Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over Gurevich et al. (U.S. patent application publication No. 2002/0178370 A1) in view of Dolan et al. (U.S. patent No. 5,604,801) as applied to claims 1-10, 13, 16-18, 20, and 22-23 above, and further in view of Kaufman et al. (U.S. patent No. 5,418,854).

As to claim 19, Gurevich et al. as modified, does not teach wherein the computer memory calculates the first number by performing a logical exclusive OR of the private key and the random number.

Kaufman et al. teaches wherein the computer memory calculates the first number by performing a logical exclusive OR of the private key and the random number (see column 3, lines 28-53).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Gurevich et al. as modified, to include wherein the computer memory calculates the first number by performing a

logical exclusive OR of the private key and the random number.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Gurevich et al. as modified, by the teachings of Kaufman et al. because wherein the computer memory calculates the first number by performing a logical exclusive OR of the private key and the random number would make it impossible for an imposter to distinguish between a successful and an unsuccessful attempt of decrypting the first component (see Kaufman et al., column 3, lines 48-53).

13. Claims 21 and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gurevich et al. (U.S. patent application publication No. 2002/0178370 A1) in view of Dolan et al. (U.S. patent No. 5,604,801) as applied to claims 1-10, 13, 16-18, 20, and 22-23 above, and further in view of Grimmer (U.S. patent No. 5,774,552).

As to claim 21, Gurevich et al. as modified, teaches wherein registering the wrapped version of the first number with the remote key server further includes:

transmitting the wrapped version of the first number to the remote key server (see Gurevich et al., page 6 paragraph 0068 line 13-18);

Gurevich et al. as modified does not teach transmitting a user name to the key server; and transmitting a second hash value to the key server, the second hash value being based on the password, the user name, and a second fixed random number.

Grimmer teaches transmitting a user name to the key server (see column 4, line

63 through column 5, line 7); and transmitting a second hash value to the key server, the second hash value being based on the password, the user name, and a second fixed random number (see column 4, lines 57-62).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Gurevich et al. as modified, to include transmitting a user name to the key server; and transmitting a second hash value to the key server, the second hash value being based on the password, the user name, and a second fixed random number.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Gurevich et al. as modified, by the teachings of Grimmer because transmitting a user name to the key server; and transmitting a second hash value to the key server, the second hash value being based on the password, the user name, and a second fixed random number would give a simple form of protected authentication (see column 4, lines 53-62).

As to claim 24, Gurevich et al. as modified, teaches wherein registering the wrapped version of the first number with the remote key server further includes:

transmitting the wrapped version of the first number to the remote key server (see Gurevich et al., page 6, paragraph 0068, line 13-18);

Gurevich et al. as modified, does not teach transmitting a user name to the key server; and transmitting a second hash value to the key server, the second hash value being based on the password, a user name, and a second fixed random number.

Grimmer teaches transmitting a user name to the key server (see column 4, line 63 through column 5, line 7); and transmitting a second hash value to the key server, the second hash value being based on the password, a user name, and a second fixed random number (see column 4, lines 57-62).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Gurevich et al. as modified, to include transmitting a user name to the key server; and transmitting a second hash value to the key server, the second hash value being based on the password, a user name, and a second fixed random number.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Gurevich et al. as modified, by the teachings of Grimmer because transmitting a user name to the key server; and transmitting a second hash value to the key server, the second hash value being based on the password, a user name, and a second fixed random number would give a simple form of protected authentication (see column 4, lines 53-62).

14. Claims 25-28 rejected under 35 U.S.C. 103(a) as being unpatentable over Gurevich et al. (U.S. patent publication No. 2002/0178370 A1) in view of Kaufman et al. (U.S. patent No. 5,418,854).

As to claim 25, Gurevich et al. teaches a distributed data object stored on a plurality of computers (see figure 1), the distributed data object comprising:

a second component, the second component being wrapped with the encryption key and stored on a client computer of the plurality of computers (see page 6, paragraph 0068).

Gurevich et al. does not teach a first component, the first component being wrapped with an encryption key based on a hash value that is based on a user password, the first component being stored on a key server computer of the plurality of computers; wherein the first and second components of the data object, when unwrapped with the encryption key and combined using a logical exclusive OR operation, generate a private key in a public/private key encryption pair for a user of the client computer.

Kaufman et al. teaches a first component, the first component being wrapped with an encryption key based on a hash value that is based on a user password, the first component being stored on a key server computer of the plurality of computers; wherein the first and second components of the data object, when unwrapped with the encryption key and combined using a logical exclusive OR operation, generate a private key in a public/private key encryption pair for a user of the client computer (see column 3, lines 28-53).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Gurevich et al. to include a first component, the first component being wrapped with an encryption key based on a hash value that is based on a user password, the first component being stored on a key server computer of the plurality of computers; wherein the first and second components

of the data object, when unwrapped with the encryption key and combined using a logical exclusive OR operation, generate a private key in a public/private key encryption pair for a user of the client computer.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Gurevich et al. by the teachings of Kaufman et al. because a first component, the first component being wrapped with an encryption key based on a hash value that is based on a user password, the first component being stored on a key server computer of the plurality of computers; wherein the first and second components of the data object, when unwrapped with the encryption key and combined using a logical exclusive OR operation, generate a private key in a public/private key encryption pair for a user of the client computer would make it impossible for an imposter to distinguish between a successful and an unsuccessful attempt of decrypting the first component (see Kaufman et al., column 3, lines 48-53).

As to claim 26, Gurevich et al. as modified, teaches wherein the first component is calculated from the private key and the second component (see Kaufman et al., column 3, lines 43-47).

As to claim 27, Gurevich et al. as modified, teaches wherein the first component is calculated as the logical exclusive OR of the private key and the second component (see Kaufman et al., column 3, lines 43-47).

As to claim 28, Gurevich et al. as modified, teaches wherein the second component is a random number (see Gurevich et al., page 6, paragraph 0068, lines 3-6).

Conclusion

15. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jacob F. Betit whose telephone number is (703) 305-3735. The examiner can normally be reached on Monday through Friday 9 am to 5 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Dov Popovici can be reached on (703) 305-3830. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

DOV POPOVICI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

jfb
February 6, 2004